

PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro



INTERNATIONALE ANMELDUNG VERÖFFENTLICH NACH DEM VERTRAG ÜBER DIE
INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 : G07F 7/10, G07C 9/00	A1	(11) Internationale Veröffentlichungsnummer: WO 00/60551
		(43) Internationales Veröffentlichungsdatum: 12. Oktober 2000 (12.10.00)

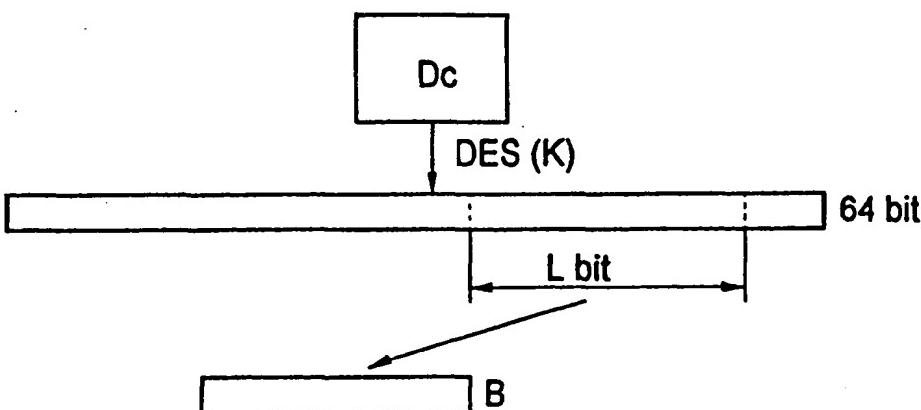
(21) Internationales Aktenzeichen: PCT/EP00/02481	(81) Bestimmungsstaaten: AU, CA, JP, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).
(22) Internationales Anmeldedatum: 21. März 2000 (21.03.00)	
(30) Prioritätsdaten: 199 14 407.9 30. März 1999 (30.03.99) DE	Veröffentlicht <i>Mit internationalem Recherchenbericht. Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.</i>
(71) Anmelder (für alle Bestimmungsstaaten ausser US): DEUTSCHE TELEKOM AG [DE/DE]; Friedrich-Ebert-Allee 140, D-53113 Bonn (DE).	
(72) Erfinder; und	
(75) Erfinder/Anmelder (nur für US): SCHWENK, Jörg [DE/DE]; Südwestring 27, D-64807 Dieburg (DE). MARTIN, Tobias [DE/DE]; Spitzengärten 1, D-35466 Rabenau-Ruddinghausen (DE).	
(74) Gemeinsamer Vertreter: DEUTSCHE TELEKOM AG; Rechtsabteilung (Patente) PA1, D-64307 Darmstadt (DE).	

(54) Title: METHOD OF DERIVING AN IDENTIFICATION NUMBER

(54) Bezeichnung: VERFAHREN ZUR ABLEITUNG VON IDENTIFIKATIONSNUMMERN

(57) Abstract

The invention relates to a method of deriving a personal identification number (PIN) that consists of a number N of decimal digits, for use of credit cards and other safety-requiring devices, from a binary number of L decimals, especially a binary code that is specific of a person. According to the inventive method, the PINs are generated in such a manner that they have a statistically even distribution over the available range of numbers.



(57) Zusammenfassung

Bei einem Verfahren zur Ableitung einer Personen-Identifikations-Nummer (PIN), bestehend aus einer Anzahl N dezimaler Ziffern, zur Benutzung von Geldkarten und anderen sicherheitsbedürftigen Einrichtungen aus einer binären Zahl mit L Stellen, insbesondere einem personenspezifischen Binärkode, werden die PINs so erzeugt, dass sie statistisch gleichmässig auf den zur Verfügung stehenden Zahlenbereich verteilt sind.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland	ML	Mali	TR	Türkei
BG	Bulgarien	HU	Ungarn	MN	Mongolei	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MR	Mauretanien	UA	Ukraine
BR	Brasilien	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Island	MX	Mexiko	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	NE	Niger	UZ	Usbekistan
CF	Zentralafrikanische Republik	JP	Japan	NL	Niederlande	VN	Vietnam
CG	Kongo	KE	Kenia	NO	Norwegen	YU	Jugoslawien
CH	Schweiz	KG	Kirgisistan	NZ	Neuseeland	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	PL	Polen		
CM	Kamerun	KR	Republik Korea	PT	Portugal		
CN	China	KZ	Kasachstan	RO	Rumänien		
CU	Kuba	LC	St. Lucia	RU	Russische Föderation		
CZ	Tschechische Republik	LI	Liechtenstein	SD	Sudan		
DE	Deutschland	LK	Sri Lanka	SE	Schweden		
DK	Dänemark	LR	Liberia	SG	Singapur		
EE	Estland						

Verfahren zur Ableitung von Identifikationsnummern

Die Erfindung betrifft ein Verfahren zur Ableitung einer Personen-Identifikations-Nummer (PIN), bestehend aus einer Anzahl N dezimaler Ziffern, zur Benutzung von Geldkarten und anderen sicherheitsbedürftigen Einrichtungen aus einer binären Zahl mit L Stellen, insbesondere einem personenspezifischen Binärcode.

Bei der Verwendung automatischer Geldausgabesysteme oder ähnlicher mit einer Plastikkarte zu benutzenden Einrichtungen muß sich der Benutzer häufig mittels einer nur ihm bekannten vierstelligen Nummer (PIN) autorisieren. Es gibt jedoch bei weitem nicht soviele verschiedene PINs wie Benutzer, weshalb jede PIN mehrfach existiert.

Die PINs dürfen nur dezimale Ziffern enthalten, damit sie mit numerischen Tastaturen eingegeben werden können. Ferner sollen sie nicht mit einer Null beginnen. Daraus ergibt sich bei vier Stellen ein Bereich von 9000 unterschiedlichen PINs. Die theoretisch geringstmögliche Wahrscheinlichkeit, eine PIN zu erraten, beträgt somit 1/9000.

Aufgabe der vorliegenden Erfindung ist es, ein Verfahren anzugeben, welches die Wahrscheinlichkeit möglichst gering hält, daß eine PIN erraten werden kann.

Der Erfindung liegt die Erkenntnis zugrunde, daß, wenn die PINs so erzeugt werden, daß sie statistisch gleichmäßig auf den zur Verfügung stehenden Zahlenbereich verteilt sind, die Wahrscheinlichkeit, eine PIN zu erraten, minimal wird. Dies wird anhand des folgenden Beispiels erläutert.

Aus persönlichen Daten des Benutzers kann mit einem geheimen Schlüssel unter Zuhilfenahme eines Verschlüsselungsalgorithmus ein Binärcode erzeugt werden. Bei Verwendung des beispielsweise zur Erzeugung von PINs für Geldkarten vorgesehenen DES- oder Triple-DES-Algorithmus wird mit Hilfe eines bankeigenen Schlüssels aus den Daten eines Kunden ein 64-stelliger Binärcode generiert. Aus einem Abschnitt von 16 Stellen dieses Binärcodes kann die PIN beispielsweise auf folgende Weise erzeugt werden:

Es werden vier Teile zu jeweils vier Stellen dieser binären Zahl zu vier Dezimalzahlen zusammengefaßt. Die vier Ziffern der PIN ergeben sich als Rest einer Division dieser vier Dezimalzahlen durch 10 (Modulo-Funktion). Falls die erste Ziffer eine Null ist, wird sie gegen eine Eins ausgetauscht. Die daraus resultierenden PINs sind jedoch in hohem Maße ungleichmäßig über den zur Verfügung stehenden Zahlenbereich

von 1 bis 9000 verteilt. Die Wahrscheinlichkeit, eine derartig erzeugte PIN zu erraten, ist gar höher als 1/150, falls sie mit einer 1 beginnt.

- 5 Verteilt man die PINs dagegen gleichmäßig über den Zahlenbereich, so ist die Auftretenshäufigkeit einer jeden PIN konstant 1/9000 und daher ist auch die Wahrscheinlichkeit minimal, daß sie erraten wird.
- 10 Eine erste Ausgestaltung der Erfindung sieht vor, daß die ersten n1 Stellen der binären Zahl (B) auf an sich bekannte Weise in eine Dezimalzahl d1 umgesetzt werden, wobei die vorgebbare natürliche Zahl n1 so gewählt wird, daß es eine derartige natürliche Zahl z1 gibt, daß der Quotient
- 15 $2^{n1}/(z1*9)$ nahe bei 1 liegt, und daß die erste Dezimalziffer der PIN den Wert d1 Modulo 9 erhält, daß N-1 weitere Gruppen von jeweils weiteren n2 Stellen der binären Zahl (B) auf an sich bekannte Weise in N-1 Dezimalzahlen d2 bis dN umgesetzt werden, wobei die vorgebbare Zahl n2 so gewählt wird, daß es
- 20 eine derartige natürliche Zahl z2 gibt, daß der Quotient $2^{n2}/(z2*10)$ nahe bei 1 liegt, der Bedingung genügen soll: $0 \leq 2^{n2} \text{ Modulo } 10 < 3$, und daß die Dezimalziffern 2 bis N der PIN die Werte di Modulo 10, i=2 bis N erhalten.
- 25 Zur Erzeugung der ersten Ziffer der PIN wird n1 so gewählt, daß 2^{n1} in der Nähe eines Vielfachen von 9 liegt. Der vornstehende n1-stellige Teil der binären Zahl wird als Dezimalzahl interpretiert. Es wird der ganzzahlige Rest bei einer Division durch 9 ermittelt. Dieser Rest bildet die
- 30 erste Ziffer der PIN. Zur Erzeugung der Ziffern 2 und folgende der PIN werden je n2 bits abgespalten. Die Zahl n2 ist so gewählt, daß 2^n in der Nähe eines Vielfachen von 10 liegt. Die resultierende Zahl wird als Dezimalzahl interpretiert. Es wird der ganzzahlige Rest bei einer
- 35 Division durch 10 ermittelt. Dieser Rest bildet die jeweilige Ziffer der PIN. Hierdurch ergibt sich zwar keine absolute Gleichverteilung. Die PIN-Ziffern sind aber umso gleichmäßiger verteilt, je größer n2 ist.
- 40 Wird beispielsweise n2=13 gewählt, so ergibt sich ein Zahlenbereich von 1 bis $2^{13}=8192$. Die Ziffern 0, 1, 2 und 3 treten in den erzeugten PINs mit einer Wahrscheinlichkeit von 820/8192 und die restlichen Ziffern mit einer Wahrscheinlichkeit von 819/8192 auf. Insbesondere wird bei
- 45 dem erfindungsgemäßen Verfahren vermieden, daß die 1 in der ersten Stelle der PIN übermäßig häufig auftritt.

Bei einer Weiterbildung der Erfindung ist vorgesehen, daß n1 und $n2 \leq 16$ vorgegeben werden.

Bei einer nächsten Weiterbildung der Erfindung ist vorgesehen, daß N=4 gewählt wird.

Es kann ferner vorgesehen sein, daß die binäre Zahl (B) die 5 Länge L=16 aufweist, daß N=4 vorgegeben wird und daß n1=n2=4 vorgegeben werden.

Eine andere Ausgestaltung der Erfindung besteht darin, daß 10 die binäre Zahl (B) die Länge L=3*n3 aufweist, daß n3 Gruppen von jeweils drei Stellen der binären Zahl (B) auf an sich bekannte Weise zur Bildung der Ziffern der PIN in n3 Dezimalziffern umgesetzt werden, wobei n3 eine natürliche Zahl ist. Bei dieser Variante werden insgesamt 12 bit des 15 kundenspezifischen Binärcodes zur Erzeugung der PIN benutzt. Je 3 bit dieser Binärzahl werden als Dezimalziffer zwischen 1 und 8 interpretiert. Die damit erzeugten PINs sind absolut gleichmäßig verteilt.

Eine weitere Möglichkeit, innerhalb des jeweiligen 20 Zahlenbereiches absolut gleichverteilte PINs zu erzeugen, besteht darin, daß die binäre Zahl zur Bildung der PIN in an sich bekannter Weise komplett in eine Dezimalzahl umgesetzt wird und daß zu der sich ergebenden Dezimalzahl erforderlichenfalls ein derartiger Korrekturwert hinzugaddiert 25 wird, daß die erste Ziffer der Dezimalzahl ungleich Null wird, wobei die Ziffern des Ergebnisses die Ziffern der PIN bilden.

Es kann dazu vorgesehen sein, daß die Länge L der binären 30 Zahl 13 beträgt, daß die erzeugte Dezimalzahl vier Stellen aufweist und daß zu der Dezimalzahl ein fest vorgegebener Wert größer als 999 und kleiner als 1807 hinzugaddiert wird, oder daß die Länge L der binären Zahl 16 beträgt, daß die 35 erzeugte Dezimalzahl fünf Stellen aufweist und daß zu der Dezimalzahl ein fest vorgegebener Wert größer als 9999 und kleiner als 34465 hinzugaddiert wird.

Im ersten Fall (L=13) kann ferner vorgesehen sein, daß die Menge der Zahlen 0 bis 8191 in n5 Teilmengen M₁,...,M_{n5} 40 aufgeteilt wird und daß der erzeugten Dezimalzahl, wenn sie ein Element der Menge M_i ist, ein fest vorgegebener Wert hinzugaddiert wird, wobei gilt 999< d₁< d₂<...< d_{n5}< 1809 und wobei n5 eine natürliche Zahl ist.

45 Im zweiten Fall (L=16) kann ferner vorgesehen sein, daß die Menge der Zahlen 0 bis 65535 in n5 Teilmengen M₁,...,M_{n5} aufgeteilt wird und daß der erzeugten Dezimalzahl, wenn sie ein Element der Menge M_i ist, ein fest vorgegebener Wert hinzugaddiert wird, wobei gilt 9999< d₁< d₂<...< d_{n5}< 34465 und 50 wobei n5 eine natürliche Zahl ist.

Eine weitere vorgeschlagene Ausgestaltung der Erfindung besteht darin, daß zur Erstellung der ersten Ziffer der PIN folgende Schritte ausgeführt werden:

- aus der binären Zahl (B) der Länge L wird eine Pseudo-Zufallszahl generiert, welche aus bis zu 36 hexadezimalen Ziffern besteht,
- jede hexadezimale Ziffer dieser Zahl wird mit jeweils einer unterschiedlichen der 36 möglichen mathematischen Abbildungen hexadezimaler Ziffern in die Ziffern 1 bis 9 in eine Ziffer aus den Ziffern von 1 bis 9 umgesetzt,
- die bis zu 36 dezimalen Ziffern der somit erzeugten Zahl werden zur Vergleichmäßigung der Auftretenswahrscheinlichkeit der jeweiligen Ziffer der PIN durch eine mathematische Operation miteinander zu einer dezimalen Ziffer ungleich Null verknüpft, welche die erste Ziffer der PIN darstellt,

und daß folgende Schritte jeweils für die zweite und jede folgende Ziffer der zu erstellenden PIN ausgeführt werden:

- aus der binären Zahl (B) der Länge L wird eine Pseudo-Zufallszahl generiert, welche aus bis zu 210 hexadezimalen Ziffern besteht,
- jede hexadezimale Ziffer dieser Zahl wird mit jeweils einer unterschiedlichen der 210 möglichen mathematischen Abbildungen hexadezimaler Ziffern in dezimale Ziffern in eine dezimale Ziffer umgesetzt,
- die bis zu 210 dezimalen Ziffer der somit erzeugten Zahl werden zur Vergleichmäßigung der Auftretenswahrscheinlichkeit der jeweiligen Ziffer der PIN durch eine mathematische Operation miteinander zu einer dezimalen Ziffer verknüpft, welche die jeweilige Ziffer der PIN darstellt.

Dazu kann vorgesehen sein, daß die erste Ziffer der PIN gebildet wird, indem die bis zu 36 Ziffern mit der Gruppenoperation einer beliebigen mathematischen Gruppe der Ordnung 9 verknüpft werden und daß die zweite und die folgenden Ziffern der PIN gebildet werden, indem die jeweils bis zu 210 Ziffern mit der Gruppenoperation einer beliebigen mathematischen Gruppe der Ordnung 10 verknüpft werden.

Bei dieser Ausgestaltung des erfindungsgemäßen Verfahrens wird aus N Gruppen von jeweils 4 bit Länge je eine Hexadezimalzahl gebildet. Diese soll nun in eine Dezimalziffer umgesetzt werden. Für diese Umsetzung stehen insgesamt $(10 \text{ über } 6) = (10 \text{ über } 4) = 210$ unterschiedliche Abbildungen der hexadezimalen Ziffern in die Menge der dezimalen Ziffern zur Verfügung. Eine mögliche Abbildung ist die Bildung des Rests bei der Division durch 10: $(0 \rightarrow 0, 1 \rightarrow 1, 2 \rightarrow 2, 3 \rightarrow 3, 4 \rightarrow 4, 5 \rightarrow 5, 6 \rightarrow 6, 7 \rightarrow 7, 8 \rightarrow 8, 9 \rightarrow 9, A \rightarrow 0, B \rightarrow 1, C \rightarrow 2, D \rightarrow 3, E \rightarrow 4, F \rightarrow 5)$. Nach

dieser Abbildung treten die Ziffern 0 bis 5 jeweils mit der Häufigkeit von 1/8 und die Ziffern von 6 bis 9 mit der Häufigkeit 1/16 auf. Um nun Ziffern zu erhalten, deren Auftretenswahrscheinlichkeit nicht oder unmerklich von 1/10 abweicht, wird vorgeschlagen, die 210 Hexadezimalziffern, die beispielsweise durch 14-maliges Anwenden des o.g. DES-Algorithmus auf die 64-stellige binäre Ausgangszahl erzeugt wurden (daher Pseudo-Zufallszahl, da die erzeugte Zahl mitnichten zufällig entstanden ist), mit je einer anderen der 210 möglichen Abbildungen in eine Dezimalziffer umzusetzen und anschließend alle 210 Dezimalziffern mit einer Gruppenoperation einer mathematischen Gruppe mit zehn Elementen zu einer einzigen Ziffer zu verknüpfen. Die Auftretenswahrscheinlichkeit jeder so erzeugten dezimalen Ziffer liegt nahe bei 1/10.

Es ist bei einer nächsten Weiterbildung der Erfindung vorgesehen, daß die additive Gruppe der ganzen Zahlen Modulo 10 zur Verknüpfung der bis zu 210 Ziffern verwendet wird. Es werden dabei jeweils 210 Dezimalziffern zu einer einzigen Ziffer verknüpft, indem man alle Ziffern addiert und den Rest einer Division der Summe durch 10 als Ergebnis nimmt. Die dabei auftretenden zehn möglichen Ergebnisse sind die Elemente der additiven Gruppe $Z_{10, +}$.

Bei einer anderen Weiterbildung der Erfindung ist vorgesehen sein, daß die multiplikative Gruppe der ganzen Zahlen Modulo 11 zur Verknüpfung der bis zu 210 Ziffern verwendet wird. Diese Gruppe Z_{11}^* weist ebenfalls zehn Elemente auf und eignet sich daher zur Verknüpfung der Zahlen zu einer Dezimalziffer. In Z_{11}^* rechnet man, indem man zwei Elemente multipliziert und das Ergebnis durch 11 dividiert. Der dabei bleibende Rest bildet das Ergebnis der Operation. Die Null ist aus der Gruppe ausgenommen. Die in den Ziffern auftretende 0 indiziert das Element Nr. 10 der Gruppe Z_{11}^* .

Eine andere Weiterbildung der Erfindung sieht vor, daß die Gruppe der Symmetrieabbildungen eines regelmäßigen Fünfecks (Diedergruppe) zur Verknüpfung der bis zu 210 Ziffern verwendet wird, wobei jeder der zehn Symmetrieabbildungen dieser Gruppe eine andere dezimale Ziffer zugeordnet wird. Dazu kann ferner vorgesehen sein, daß der Identitätsabbildung die Ziffer 0, den vier Drehungen um den Mittelpunkt des Fünfecks die Ziffern 1 bis 4 und den fünf Spiegelungen um die fünf Symmetrieeachsen des Fünfecks die Ziffern 5 bis 9 zugeordnet werden. Führt man zwei Symmetrieabbildungen hintereinander aus, so entsteht wieder eine Symmetrieabbildung. Es läßt sich mit diesen Zuordnungen die folgende Multiplikationstabelle aufstellen:

*	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	6	7	8	9	5
5	2	3	4	0	1	7	8	9	5	6
	3	3	4	0	1	2	8	9	5	6
	4	4	0	1	2	3	9	5	6	7
	5	5	9	8	7	6	0	4	3	2
10	6	6	5	9	8	7	1	0	4	3
	7	7	6	5	9	8	2	1	0	4
	8	8	7	6	5	9	3	2	1	0
20	9	9	8	7	6	5	4	3	2	1
										0.

Die 210 Ziffern werden mit Hilfe dieser Tabelle zu einer einzigen Ziffer verknüpft, indem sukzessiv mit dem Ergebnis der letzten Operation als Zeilenindikator und mit der nächsten Ziffer als Spaltenindikator das nächste Ergebnis in der Tabelle abgelesen wird, bis alle Ziffern berücksichtigt wurden. Das letzte Ergebnis bildet die gesuchte Ziffer der PIN.

Ausführungsbeispiele der Erfindung sind in der Zeichnung anhand mehrerer Figuren dargestellt und in der nachfolgenden Beschreibung näher erläutert. Es zeigt:

- 25 Fig. 1 ein Diagramm zur Erzeugung eines kundenspezifischen Binärcodes,
- 30 Fig. 2 ein Diagramm zur Erzeugung einer PIN durch Umwandlung in eine Dezimalzahl,
- Fig. 3 ein Diagramm zur Erzeugung einer PIN durch ziffernweise Umwandlung in Dezimalzahlen,
- 35 Fig. 4 ein Diagramm zur Erzeugung einer PIN durch ziffernweise Umsetzung mit Modulbildung und
- Fig. 5 ein Diagramm zur Erzeugung einer PIN durch Reduktion von Hexadezimalzahlen mit Hilfe mathematischer Gruppen.

Gleiche Teile sind in den Figuren mit gleichen Bezugszeichen versehen.

- 45 Fig. 1 zeigt ein Ablaufdiagramm zur Umsetzung von persönlichen Daten Dc eines Kunden mit Hilfe eines geheimen Schlüssels K in eine binäre Zahl B von L bit Länge. Die binäre Zahl B ist Teil des 64 bit langen Verschlüsselungsergebnisses, welches aus den Kundendaten Dc mit dem DES-Algorithmus erzeugt wurde.

Sei die Länge der binären Zahl B gleich 13 und sei die Anzahl der zu erzeugenden Ziffern der PIN gleich 4, so kann die PIN, wie in Fig. 2 gezeigt wird, dadurch erzeugt werden, daß die 5 binäre Zahl B als Dezimalzahl D interpretiert und dazu eine Konstante C addiert wird. Die Konstante ist so zu wählen, daß die PIN keine führenden Nullen aufweist. Auf diese Weise können 8192 unterschiedliche PINs erzeugt werden, die über den jeweiligen Zahlenbereich absolut gleichmäßig verteilt 10 sind.

Fig. 3 zeigt, wie eine binäre Zahl der Länge 13 in eine PIN umgewandelt werden kann, indem man je Ziffer der zu erzeugenden PIN eine Anzahl bits der binären Zahl in eine 15 Dezimalzahl umwandelt und zu der sich daraus ergebenden Zahl D eine Konstante C addiert, um führende Nullen der PIN zu vermeiden. Auf diese Weise können 7777 unterschiedliche PINs erzeugt werden, die über dem jeweiligen Zahlenbereich absolut gleichmäßig verteilt sind.

20 Eine weitere Möglichkeit zur Erzeugung annähernd gleich verteilter PINs aus einer binären Zahl B ist in Fig. 4 dargestellt. Die binäre Zahl B habe 52 Stellen. Zur Erzeugung der vierstelligen PIN wird die binäre Zahl B in vier Teile 25 unterteilt, die im Beispiel die gleiche Länge haben. Jedes dieser Teile wird als Dezimalzahl interpretiert. Die erste Ziffer der PIN ergibt sich als Rest einer Division der ersten Dezimalzahl durch 9. Die folgenden Ziffern der PIN ergeben sich jeweils als Rest der Division der folgenden 30 Dezimalzahlen durch 10. Auf diese Weise können 9000 unterschiedliche PINs erzeugt werden, die absolut gleichmäßig verteilt sind.

Aus den persönlichen Daten Dc eines Kunden werden, wie in 35 Fig. 5 gezeigt, mit Hilfe eines geheimen Schlüssels und eines Zufallszahlen-Generators eine Folge von 210 Hexadezimalziffern erzeugt, indem beispielsweise ein Verschlüsselungsergebnis des DES-Algorithmus aus Fig. 1 wiederum mit dem Algorithmus verschlüsselt wird und so fort. 40 Die daraus resultierenden 14 64-stelligen Binärcodes werden in 14 Hexadezimalzahlen Hi mit je 16 Stellen gewandelt. Aneinandergehängt gibt das 224 Hexadezimalziffern, wovon 210 in die Erzeugung der PIN eingehen.

45 Es gibt 210 unterschiedliche Möglichkeiten fi, die Menge der 16 Hexadezimalziffern in die Menge der 10 Dezimalziffern abzubilden. Jede der 210 Hexadezimalziffern wird daher mit einer anderen dieser Abbildungen in eine Dezimalziffer di umgesetzt. Um aus den 210 Dezimalziffern eine Ziffer Zi einer 50 PIN zu erzeugen, werden diese mit Hilfe der Gruppenoperation

F einer beliebigen zehnlementigen mathematischen Gruppe nacheinander verknüpft; das letzte Ergebnis ist die gesuchte Ziffer. Die vorher ungleichmäßige statistische Verteilung der 210 Dezimalziffern wird damit vergleichmäßig. Der gesamte 5 Vorgang wird für jede der Stellen Z2 bis Z4 der PIN erneut durchgeführt.

Für die erste Ziffer der PIN werden analog 36 Hexadezimalziffern erzeugt, die mit je einer anderen der 36 10 möglichen Abbildungen der Hexadezimalziffern in die Menge der Ziffern 1 bis 9 in eine Ziffer zwischen 1 und 9 abgebildet werden. Die 36 Dezimalziffern werden mit der Gruppenoperation einer beliebigen mathematischen Gruppe der Ordnung 9 zu der ersten Ziffer der PIN verknüpft. Es lassen sich damit 9000 15 unterschiedliche PINs erzeugen, die annähernd gleichmäßig verteilt sind. Bei der Erzeugung von 10^5 PINs betragen die maximalen Ungleichmäßigkeiten etwa 1,5 Prozent, was die Wahrscheinlichkeit, daß eine PIN zufällig erraten wird, nicht nennenswert gegenüber dem theoretischen Minimalwert erhöht. 20 Das Verfahren arbeitet damit sehr zuverlässig.

Zur Anwendung in diesem Verfahren eignen sich grundsätzlich alle mathematischen Gruppen, die zehn Elemente aufweisen. Bekannte Vertreter sind die additive Gruppe der ganzen Zahlen 25 Modulo 10, $\mathbb{Z}_{10,+}$, die multiplikative Gruppe der ganzen Zahlen Modulo 11, \mathbb{Z}_11^* , sowie die Gruppe der Symmetriearabbildungen eines regelmäßigen Fünfecks D5, die sogenannte Diedergruppe. Im letzten Falle wird den einzelnen Elementen der Gruppe je eine Dezimalziffer zugeordnet, mit der sich rechnen läßt.

Ansprüche

1. Verfahren zur Ableitung einer Personen-Identifikations-Nummer (PIN), bestehend aus einer Anzahl N dezimaler Ziffern, zur Benutzung von Geldkarten und anderen sicherheitsbedürftigen Einrichtungen aus einer binären Zahl mit L Stellen, insbesondere einem personenspezifischen Binärcode, dadurch gekennzeichnet, daß die PINs so erzeugt werden, daß sie statistisch gleichmäßig auf den zur Verfügung stehenden Zahlenbereich verteilt sind.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die ersten n1 Stellen der binären Zahl (B) auf an sich bekannte Weise in eine Dezimalzahl d1 umgesetzt werden, wobei die vorgebbare natürliche Zahl n1 so gewählt wird, daß es eine derartige natürliche Zahl Z1 gibt, daß der Quotient $2^{n1}/(Z1*9)$ nahe bei 1 liegt, und daß die erste Dezimalziffer der PIN den Wert d1 Modulo 9 erhält, daß N-1 weitere Gruppen von jeweils weiteren n2 Stellen der binären Zahl (B) auf an sich bekannte Weise in N-1 Dezimalzahlen d2 bis dN umgesetzt werden, wobei die vorgebbare Zahl n2 so gewählt wird, daß es eine derartige natürliche Zahl Z2 gibt, daß der Quotient $2^{n2}/(Z2*10)$ nahe bei 1 liegt, der Bedingung genügen soll: $0 <= 2^{n2} \text{ Modulo } 10 < 3$, und daß die Dezimalziffern 2 bis N der PIN die Werte di Modulo 10, i=2 bis N erhalten.
3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß n1 und $n2 <= 16$ vorgegeben werden.
4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß $N=4$ gewählt wird.
- 35 5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die binäre Zahl (B) die Länge L=16 aufweist, daß $N=4$ vorgegeben wird und daß $n1=n2=4$ vorgegeben werden.
- 40 6. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die binäre Zahl (B) die Länge $L=3*n3$ aufweist, daß n3 Gruppen von jeweils drei Stellen der binären Zahl (B) auf an sich bekannte Weise zur Bildung der n3 Ziffern der PIN in n3 Dezimalziffern umgesetzt werden, wobei n3 eine natürliche Zahl ist.
- 45 7. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die binäre Zahl (B) zur Bildung der PIN in an sich bekannter Weise komplett in eine Dezimalzahl umgesetzt wird und daß zu der sich ergebenden Dezimalzahl erforderlichenfalls ein

derartiger Korrekturwert hinzuaddiert wird, daß die erste Ziffer der Dezimalzahl ungleich Null wird, wobei die Ziffern des Ergebnisses die Ziffern der PIN bilden.

- 5 8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, daß die Länge L der binären Zahl (B) 13 beträgt, daß die erzeugte Dezimalzahl vier Stellen aufweist und daß zu der Dezimalzahl ein fest vorgegebener Wert größer als 999 und kleiner als 1807 hinzuaddiert wird.
- 10 9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, daß die Menge der Zahlen 0 bis 8191 in n5 Teilmengen M₁,...,M_{n5} aufgeteilt wird und daß der erzeugten Dezimalzahl, wenn sie ein Element der Menge M_i ist, ein fest vorgegebener Wert di hinzuaddiert wird, wobei gilt 999< d₁< d₂<...< d_{n5}< 1809 und wobei n5 eine natürliche Zahl ist.
- 15 10. Verfahren nach Anspruch 7, dadurch gekennzeichnet, daß die Länge L der binären Zahl (B) 16 beträgt, daß die erzeugte Dezimalzahl fünf Stellen aufweist und daß zu der Dezimalzahl ein fest vorgegebener Wert größer als 9999 und kleiner als 34465 hinzuaddiert wird.
- 20 11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, daß die Menge der Zahlen 0 bis 65535 in n5 Teilmengen M₁,...,M_{n5} aufgeteilt wird und daß der erzeugten Dezimalzahl, wenn sie ein Element der Menge M_i ist, ein fest vorgegebener Wert di hinzuaddiert wird, wobei gilt 9999< d₁< d₂<...< d_{n5}< 34465 und wobei n5 eine natürliche Zahl ist.
- 25 12. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß zur Erstellung der ersten Ziffer der PIN folgende Schritte ausgeführt werden:
 - aus der binären Zahl (B) der Länge L wird eine Pseudo-Zufallszahl generiert, welche aus bis zu 36 hexadezimalen Ziffern besteht,
 - jede hexadezimale Ziffer dieser Zahl wird mit jeweils einer unterschiedlichen der 36 möglichen mathematischen Abbildungen hexadezimaler Ziffern in die Ziffern 1 bis 9 in eine Ziffer aus den Ziffern von 1 bis 9 umgesetzt,
 - die bis zu 36 dezimalen Ziffern der somit erzeugten Zahl werden zur Vergleichmäßigung der Auftretenswahrscheinlichkeit der jeweiligen Ziffer der PIN durch eine mathematische Operation miteinander zu einer dezimalen Ziffer ungleich Null verknüpft, welche die erste Ziffer der PIN darstellt,40 und daß folgende Schritte jeweils für die zweite und jede folgende Ziffer der zu erstellenden PIN ausgeführt werden:
- 30 45 50

- aus der binären Zahl (B) der Länge L wird eine Pseudo-Zufallszahl generiert, welche aus bis zu 210 hexadezimalen Ziffern besteht,
 - jede hexadezimale Ziffer dieser Zahl wird mit jeweils einer unterschiedlichen der 210 möglichen mathematischen Abbildungen hexadezimaler Ziffern in dezimale Ziffern in eine dezimale Ziffer umgesetzt,
 - die bis zu 210 dezimalen Ziffer der somit erzeugten Zahl werden zur Vergleichsmäßigung der Auftretenswahrscheinlichkeit der jeweiligen Ziffer der PIN durch eine mathematische Operation miteinander zu einer dezimalen Ziffer verknüpft, welche die jeweilige Ziffer der PIN darstellt.
- 15 13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, daß die erste Ziffer der PIN gebildet wird, indem die bis zu 36 Ziffern mit der Gruppenoperation einer beliebigen mathematischen Gruppe der Ordnung 9 verknüpft werden und daß die zweite und die folgenden Ziffern der PIN gebildet werden, indem die jeweils bis zu 210 Ziffern mit der Gruppenoperation einer beliebigen mathematischen Gruppe der Ordnung 10 verknüpft werden.
- 20 14. Verfahren nach Anspruch 13, dadurch gekennzeichnet, daß die additive Gruppe der ganzen Zahlen Modulo 10 zur Verknüpfung der bis zu 210 Ziffern verwendet wird.
- 25 15. Verfahren nach Anspruch 13, dadurch gekennzeichnet, daß die multiplikative Gruppe der ganzen Zahlen Modulo 11 zur Verknüpfung der bis zu 210 Ziffern verwendet wird.
- 30 16. Verfahren nach Anspruch 13, dadurch gekennzeichnet, daß die Gruppe der Symmetrieabbildungen eines regelmäßigen Fünfecks (Diedergruppe) zur Verknüpfung der bis zu 210 Ziffern verwendet wird, wobei jeder der zehn Symmetrieabbildungen dieser Gruppe eine andere dezimale Ziffer zugeordnet wird.
- 35 17. Verfahren nach Anspruch 16, dadurch gekennzeichnet, daß der Identitätsabbildung die Ziffer 0, den vier Drehungen um den Mittelpunkt des Fünfecks die Ziffern 1 bis 4 und den fünf Spiegelungen um die fünf Symmetrieachsen des Fünfecks die Ziffern 5 bis 9 zugeordnet werden.

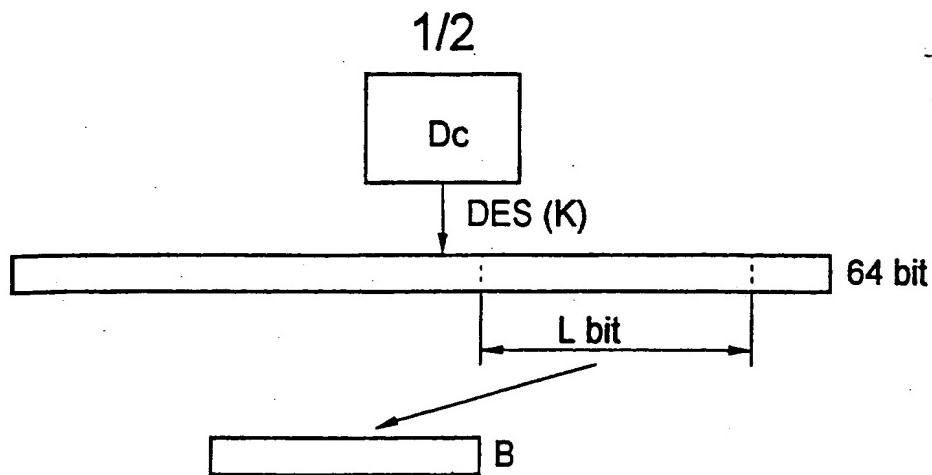


Fig.1

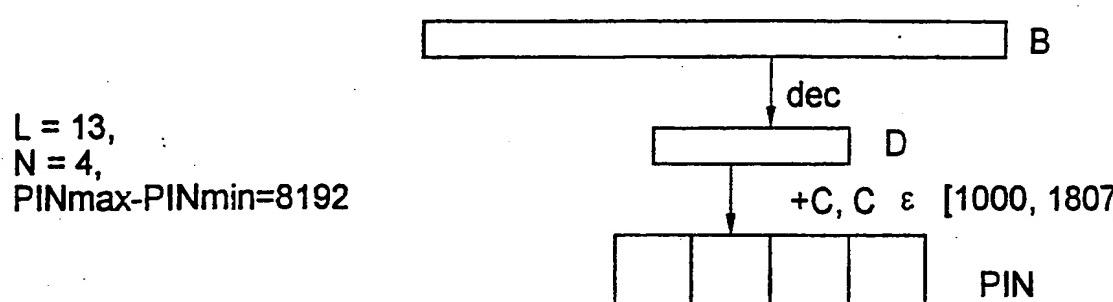


Fig.2

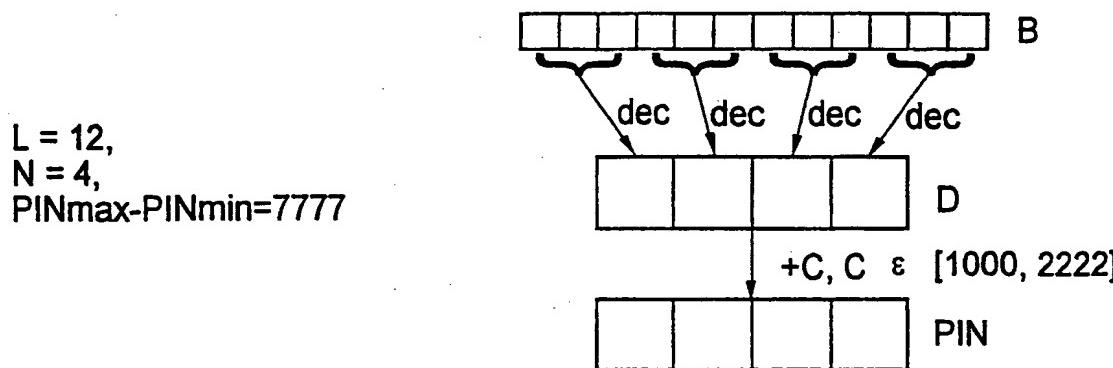


Fig.3

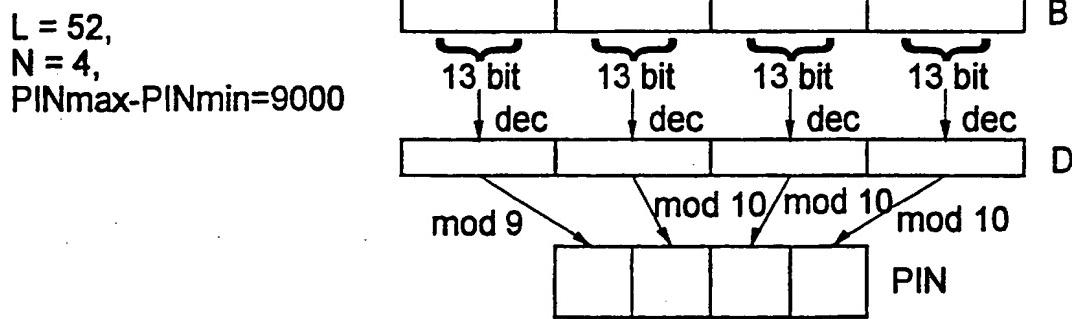


Fig.4

2/2

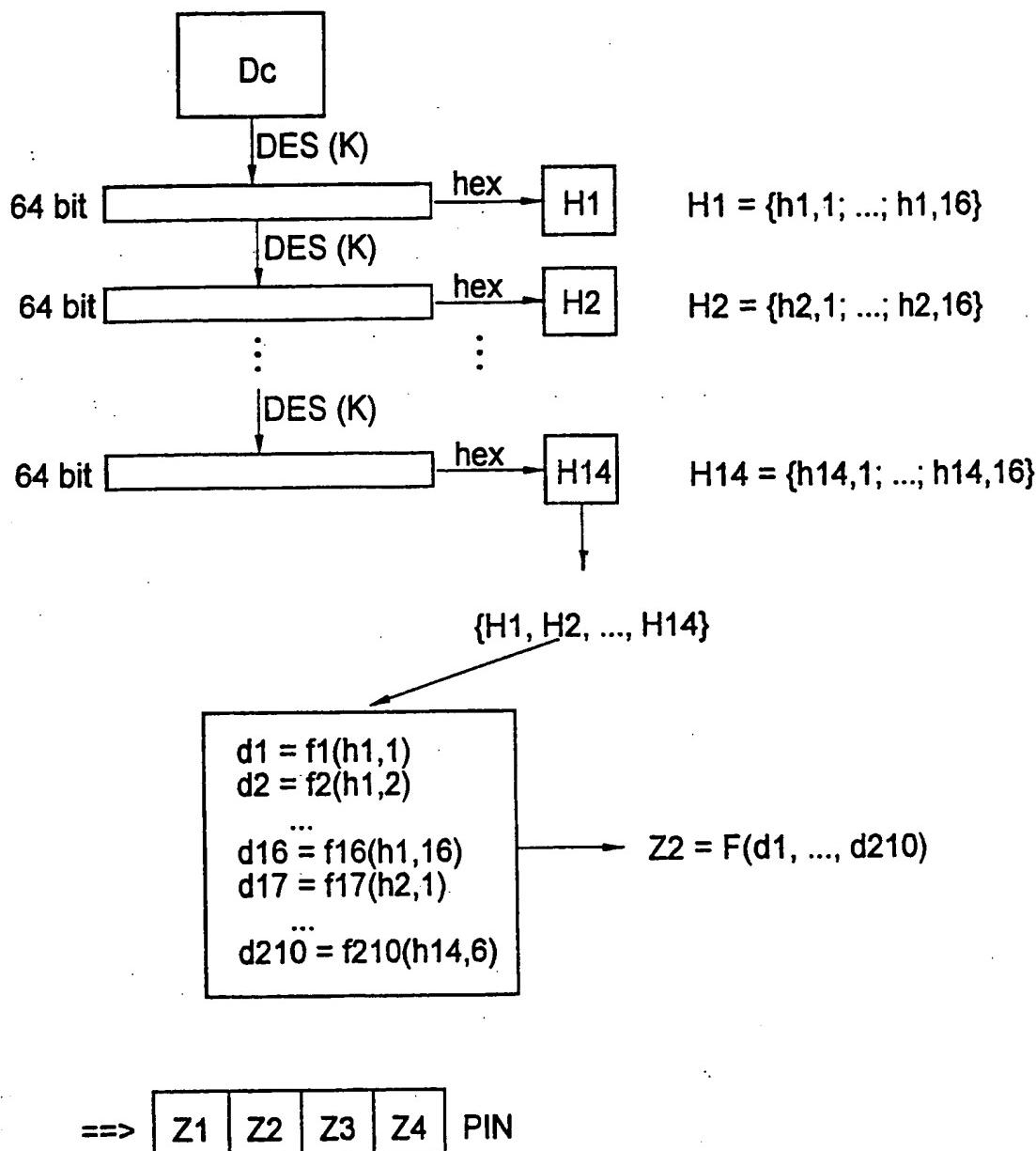


Fig.5

INTERNATIONAL SEARCH REPORT

National Application No
PCT/EP 00/02481

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10 G07C9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G07F G07C H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

WPI Data, EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	FR 2 577 704 A (SYSTÈMES SUD) 22 August 1986 (1986-08-22)	1
A	abstract; claims; figures 1,4,9 page 12, line 22 -page 15, line 17	4-6
A	US 4 605 820 A (C.M. CAMPBELL) 12 August 1986 (1986-08-12)	
A	US 3 846 622 A (M.R. MEYER) 5 November 1974 (1974-11-05)	
A	EP 0 798 891 A (MITSUBISHI DENKI) 1 October 1997 (1997-10-01)	

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

22 August 2000

Date of mailing of the international search report

30/08/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5618 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

David, J

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 00/02481

Patent document cited in search report	Publication date	Patent family member(s)			Publication date
FR 2577704	A 22-08-1986	NONE			
US 4605820	A 12-08-1986	NONE			
US 3846622	A 05-11-1974	NONE			
EP 0798891	A 01-10-1997	JP 9270053 A		14-10-1997	
		CA 2192515 A		30-09-1997	
		US 5996111 A		30-11-1999	

INTERNATIONALER RECHERCHENBERICHT

tionales Aktenzeichen

PCT/EP 00/02481

A. Klassifizierung des Anmeldungsgegenstandes
IPK 7 G07F7/10 G07C9/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationsymbole)

IPK 7 G07F G07C H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der Internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

WPI Data, EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	FR 2 577 704 A (SYSTÈMES SUD) 22. August 1986 (1986-08-22)	1
A	Zusammenfassung; Ansprüche; Abbildungen 1,4,9 Seite 12, Zeile 22 -Seite 15, Zeile 17	4-6
A	US 4 605 820 A (C.M. CAMPBELL) 12. August 1986 (1986-08-12)	
A	US 3 846 622 A (M.R. MEYER) 5. November 1974 (1974-11-05)	
A	EP 0 798 891 A (MITSUBISHI DENKI) 1. Oktober 1997 (1997-10-01)	

Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem Internationalen Anmeldeatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeschürt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem Internationalen Anmeldeatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem Internationalen Anmeldeatum oder dem Prioritätsatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzipes oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erforderlicher Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erforderlicher Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der Internationalen Recherche

Abendatum des Internationalen Recherchenberichts

22. August 2000

30/08/2000

Name und Postanschrift der Internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

David, J

INTERNATIONALES RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 00/02481

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
FR 2577704 A	22-08-1986	KEINE	
US 4605820 A	12-08-1986	KEINE	
US 3846622 A	05-11-1974	KEINE	
EP 0798891 A	01-10-1997	JP 9270053 A CA 2192515 A US 5996111 A	14-10-1997 30-09-1997 30-11-1999

This Page Blank (uspto)